European Commission

JRC TECHNICAL REPORTS

Eagle-eye on

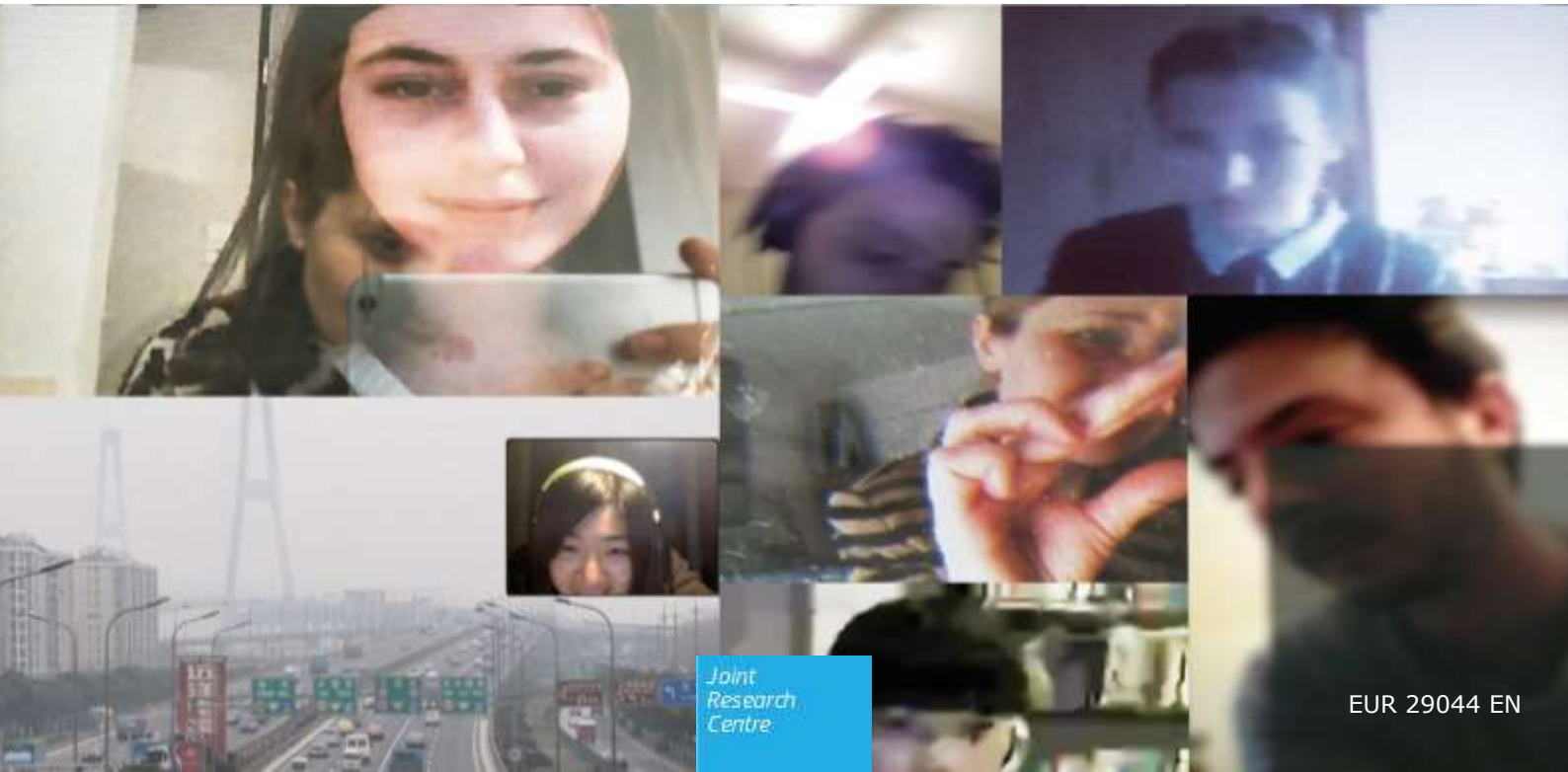
Identities in the digital world

Evolution and challenges

Stephane Chaudron

Henning Eichinger

2018



Joint Research Centre

EUR 29044 EN

JRC Science Hub
https://ec.europa.eu/jrc

JRC 110266

EUR 29044 EN

PDF	ISBN 978-92-79-77689-2	ISSN 1831-9424	doi:10.2760/48837
Print	ISBN 978-92-79-77690-8	ISSN 1018-5593	doi:10.2760/365541

Luxembourg: Publications Office of the European Union, 2018

How to cite this report: Chaudron, S. and Eichinger, H., *Eagle-eye on Identities in the digital world* , EUR 29044 EN, Publications Office of the European Union, Luxembourg, 2018, ISBN 978-92-79-77689-2, doi:10.2760/48837, JRC110266.

Contents

Acknowledgements

Although this work is mainly the result of a desk based research, it benefited from the input and collaboration of many colleagues. We are particularly grateful to Igor Nai-Fovino for showing us the way in this task, Rosanna Di Gioia, Alberto Pizzirani, Ignacio Sanchez for the work we undertook recently on privacy which nourished my reflexion on our digital identities and considerations on their protection.

Another source of inspiration to study deeper Digital Identities of the Internet Connected object was my collaboration with the co-authors of the 'Kaleidoscope on the Internet of Toys: Safety, security, privacy and societal insights'. I warmly thank Rosanna Di Gioia (JRC), Monica Gemo (JRC), Dr Donnell Holloway (Edith Cowan University, Australia), Dr Giovanna Mascheroni (Università del Sacro Cuore di Milano, Italy), Professor Jochen Peter (University of Amsterdam), Dr Dylan Yamada Rice (Dubit, UK) and Professor Jackie Marsh (University of Sheffield, UK), coordinator of the COST Action IS1410, Digital Literacy and Multimodal Practices Of Young Children (DigiLitEY) in the framework of which we started our collaboration.

Moreover, I would like to thank my colleagues Jutta Thielen - Del Pozo and Adriaan Eeckels for giving me the opportunity to meet Professor Henning Eichinger from the Fine Art, School of Textiles & Design of Reutlingen University in the preparation of the Resonances Festival 2019. Finally, but not least, I would like to express my gratitude to Henning Eichinger for accepting with enthusiasm to frame this report with an account of the artistic process of the Skypelab project that he has been leading for the last five years, searching the evolution of the portrait and the identity in the digital world with students and colleagues around the world. I thank the entire Skypelab project and its members for allowing us to illustrate this report with some of their outcomes.

Authors

Stéphane Chaudron, European Commission, Joint Research Centre

Stéphane Chaudron works on research projects dedicated to Empowering Children's Rights and Safety in emerging ICT at the Joint Research Centre of the European Commission. Her background is in Social Geography and Science Pedagogy. She has been for several years in charge of the coordination of large European Research Networks dedicated to e-Safety, New media education, Standardization and Science Teaching Education (UCLouvain, Imperial College London, European Schoolnet). She has been in charge of the coordination of EC's research project 'Young Children (0-8) and Digital Technology' since 2014. She coordinated the report 'Kaleidoscope on the Internet of Toys - Safety, security, privacy and societal insights', EUR 28397 and has since made the Internet of Toys and of Things one of her research subjects.

Report framed by

Henning Eichinger, Reutlingen University, School of Textiles & Design, Fine Art

Henning Eichinger studied Visual Communication at the University of Applied Science in Dortmund from 1980-85. As an artist and university professor, Henning Eichinger has worked for many years with themes which cross over the borders between art and science or art and technology. He investigates the intuitive and emotional components of scientific and technological developments. Since 1997 he has been professor for drawing and painting at Reutlingen University in the studies of Textile- and Fashion Design and for Fine Art Conception in the Master Program Design at Reutlingen University. In his artwork and with his students at the university he works on artistic responses to the important developments within society. Besides a number of grants, residencies and art prizes in Germany and abroad, he received in 2013 the lecture prize of the federal state of Baden-Württemberg. henning.eichinger@reutlingen-university.de - www.skypelab.org

Abstract

The concept of identity, its representation and the definition of its attributes sees essential changes in its translation into the digital world. The elements involved in the process of identification and authentication, attributes and identifiers, are created into a virtual world where physicality vanishes and elements of trust evolve, challenging the digital citizens. **How the digital world influences the construction of our identity, of our trust** is an essential question to be considered.

This report provides an bird's-eye view on the concept and implications of ***digital identities***. After an introduction situating the concept of ***identity***, the report clarifies its contemporary meaning and proposes a definition of reference. Subsequently, the authors examine the consequences of the translation of the concept of identity into the digital, internet-connected world. They then analyse the particularities and consequences of this translation, which allows them to situate and define the concept of ***digital identities***. Finally, they conclude with the **challenges** that digital identity poses to the digital citizen in the attempt to manage and protect its attributes with the advent of Internet of Things and blockchain technology.

An account by **Henning Eichinger** of the artistic process of the ***Skypelab*** project, researching the evolution on portraits and identity in the digital world since 2012 frames this report and provides a complementary perspective on the subject.

Foreword

While working on this research on the mutations of the concept of Identity in the digital world, I attended on 20 October 2017 the Preparatory workshop for the RESONANCES III Festival on Big Data at the Science and Technology Museum "Leonardo da Vinci" of Milan, and, to be honest, I did not know what to expect.

The RESONANCES Festival is part of the Joint Research Centre (JRC) SciArt - Science and Art Programme that has been launched in recent years. Indeed, the JRC, the in-house science service of the European Commission that supports policy makers with robust science, created the RESONANCE Festival as a way to boost the innovative and transdisciplinary thinking requested by increasingly complex and fast developing globalized world processes.

The first Resonances Festival was organized in 2015 as part of the EXPO 2015 in Milan on the topic of FOOD. In 2017, Resonances II addressed FAIRNESS and was presented in the JRC from 13-15 September and at the Science and Technology Museum in Milan from 21 September to 22 October.

As part of the SciArt process to prepare its 2019 edition, I had the luck to be invited along with other scientists to join up with artists to discuss, reflect, innovate, and put our research into context. The exercise aims at helping scientists to look at their research subject from different angles and other perspectives in order to, *in fine*, provide policy makers with facts as well as an encompassing and meaningful analysis.

During the day, presentations of scientist and artists alternated, followed by common and interactive discussions. The results for me were impressive and fascinating. I discovered the power of intertwined science work & artwork to foster reflections and research in unexpected areas. I also strongly felt the power of communication that mixing rationality with emotions, science with art, can create.

In this context, I discovered the ***SkypeLab*** project that researches the **changes of identity and space in a globalized and digitized world** and interprets them in an artistic way. I was delighted to meet one of its two leaders, Henning Eichinger, artist and professor at Reutlingen University, School of Textiles & Design, Fine Art who has worked for many years with themes which cross over the borders between art and science or art and technology given his interests in the intuitive and emotional components of scientific and technological developments. Having myself studied the implications of the translation of the concept of Identity into the digital world for some months already, I could not be but intrigued by the similarities between the ***SkypeLab*** project research's questions and mine **while having different approaches, reasoning and process.** But here I shall stop and leave Henning Eichinger to give you an account of ***SkypeLab***, a striking artistic project in numerous ways that frame beautifully our own report on the subject.

Stephane Chaudron

'A special drawing technique, blind contour drawing, is employed by students to draw portraits within the most varied international environments. (…) While drawing, one only looks at the object being drawn; in our project, the person on the screen opposite.', p.8.

SkypeLab 1 - Fanding Sun drawing Thi To Uyen Ly, 2015, Photography.

Report's frame - *SkypeLab*: Transcontinental Faces, Spaces and Objects - A fine art and research project about portrait and identity in a digitized world

By Henning Eichinger, Reutlingen University, School of Textiles & Design, Fine Art

***SkypeLab* - Transcontinental Faces, Spaces and Objects** is a university research project which started in March 2012 in cooperation with Professor Dr. Maggie McCormick, RMIT University Melbourne and has since enlarged to East China Normal University, Shanghai, the Institute Tercio Pacitti of Computational Applications and Research at the Federal University of Rio de Janeiro and the University of Atlántico, Barranquilla, Colombia. The focus has been to study, protocol and interpret the impacts of social networks and digital tools, by drawing portraits to investigate the nature of identity, mediated by the digital filter of Skype.

By using Skype for this drawing project between Europe, Australia, Asia and South America, *SkypeLab* researches the **changes of identity and space in a globalized and digitized world** and interprets them in an artistic way.

We deemed Skype to be the most interesting example of digital communication tools in regard to our artistic and scientific interaction. In contrast to Facebook, Instagram or other platforms, communication happens directly by seeing each other face to face, and not by proxy (such as writing, photos, avatars). Where the camera is situated - like place, interior, exterior, hints of day or night-time and season also play an important role. Geographic distance between communication partners, time lapses (Melbourne – Reutlingen – Shanghai - Rio), language and cultural differences complete the picture. These are the complex parameters of *SkypeLab.*

Portraiture and Identity

"**Identity** and **knowledge** are **increasingly shaped by seeing**, sensing and recording through digital interfaces that make Social Media the cartography of our age" [3].

In our project we see the portrait as a strong representative of one's identity, as a portrait always points beyond itself. In former times portraits were often used as representatives of sovereigns when the real person was not able to appear. Agreements and peace contracts were sealed with representing portraits. Today with social networks like Facebook, Instagram, etc. the (digital) image becomes more and more, not just a representation but a part of an individual.

One exciting area of identity is that the individual is not a set entity but develops without reaching an endpoint. We often say that the characteristics determine who we are, but we are dealing with something varying, changing, transforming, which never stands still. Identity is not something that happens to us. It is a mix between our genetics, our peer groups, environment, but also our wishes and dreams, which is an interesting accordance to social networks.

Also with the products our design students create, they produce real or seemingly real identities, or objects like accessories, that decorate or amplify identity like a filter on Instagram. When we consider identity as a combination of characteristics which distinguish

a person from others, we realise that alongside the possibility of actual identities, virtual identities also exist. Changing identities and creating new ones in the Internet, in chatrooms, communities and games is quite normal now. This is one of the fundamental changes of being human in the 21st century.

Currently, representations in the World Wide Web like avatars and made up characters allow us to happily live the various lives of a multiple-personality which probably influence who we are more than we realise. We post fragments of self-portraits every day on social media networks. Photos, texts and statements which are commented on by others, reflected upon, changed or reused. These things join together to create a virtual mosaic of our personality. In contrast to this, with our project, we wanted to show the individual artistic portrait, whether it be drawn, painted or photographed, face to face so to speak. The portrait as the centre of our identity, but also a portrait which has passed through a digital filter. We want to uncover how the layers of technology influence the perception of ourselves and others.

A Special Drawing Technique

A special drawing technique, blind contour drawing, is employed by students to draw portraits within the most varied international environments. They draw and map personalities within their living spaces in a transient world developing ever faster and further.

Blind contour drawing was developed in 1891 by Washington born Kimon Nicolaïdes an American with Greek background. In his book, "Natural Way to Draw" [1] Nicolaïdes describes the technique, which can be summarized with the following rules. While drawing, one only looks at the object being drawn; in our project, the person on the screen opposite. One is not allowed to look at or control what one is drawing under any circumstances. Normally, while drawing, one constantly looks from object to drawing to watch and control the development. Then, the drawing must be linear, without structure or shading. The pencil line must be fluid and the pencil must stay on the paper the entire time. It may not be lifted and replaced. So the lines inevitably cross over each other and create new forms. The whole process lasts about 2 - 3 minutes. Later, the educator, artist and scientist Betty Edwards from the Centre for the Educational Applications of Brain Hemisphere Research at California State University, developed the technique further along more scientific lines. In her book [2] she explains that using this technique especially stimulates the right brain hemisphere, which is responsible for intuitive, visual, spontaneous, emotional and subjective thinking. This can be proven in the drawings. They are much more lively, exciting and individual than naturalistic drawings. This fast and spontaneous way of drawing is to us a matching correspondence to our dealings with the Word Wide Web.

After a while, the portrait genre seemed to us too restricting and so we expanded the drawing communication via Skype from portrait to include space, and later on to objects which would also indicate aspects of individuality.

Questions about identity

Beyond the ubiquitous availability of information, the internet has also altered the space we communicate within. Social networks are thus virtual representations of public spaces in which we float. *SkypeLab* has been conceptualized as an open project since the very beginning to keep results unpredictable, asking questions rather than just answering them.

As this is a research based art project, the questions arising are often more important for gaining insight and artistic formation than short term results which would soon be swept away by the next wave of digital developments. Because *SkypeLab* started as an open process, rapidly compelling questions arose, such as; Is there a change of identity through communication filters? Does identity get blurred or sharpened through the screen? How can we map identity? Do we develop new feelings triggered by social networks? So, we decided to start a research Blog on our website, called 100 Questions [4].

Participants of *SkypeLab* set up frameworks for live experiments. They disguised themselves in analogy to create an avatar of their own. They staged the scene around the drawing sessions like in former times painters did through decorating the scene around a portrait to see whether that could intensify visual parts of identity by using objects and symbols. The protocol sheets filled in by the students indicated strongly that digital identity is like we said above, not out of one piece, but assembles itself like a huge mosaic from various real and digital manifestations. So, this raises further questions. Is information about us in social networks an extended part of our identity? Do they reinforce our identity or does this lead to dissociation? Can we merge our identity with others? (As some participants experimented with overlaying portraits, photos and screenshots.) Another strong feeling some described was the antithesis of feeling very close to someone through the countless and constantly updating information in the internet and then feeling alienated at the same time. They wrote and talked about the difficulty of creating a sense of a reliable and confident identity of themselves as well as of their counterparts.

Thus, *SkypeLab* links themes such as digitalisation and identity, globalisation and internationality and facilitates playfully how we grapple with these themes and how we transform our questions into artistic positions, evaluations and interpretations. So it vitalizes the debate on significant questions about identity in digitized times. Perhaps it will even help to recapture some control of interpretation of these technologies in general.

Metaphors

Unexpectedly, the screen itself played another important role in our project. As we started to take screenshots, we discovered that in the screens our portraits as our representatives not only overlaid but also crossed over into the reflections on the screen. Let me give an example. Skyping with a friend in Melbourne, I see my own screen on which there is a Skype image of my partner, while at the same time, to the bottom left, my own image displayed in miniature format. I look at the face of my Skype partner who is wearing glasses, and I see multiple layers: my own mirrored image on the screen overlapping the Skype portrait of my partner, which I can of course, see very clearly. In the lenses of my Melbourne partner's glasses, I then see further reflections. I see myself there just as my image is presented on the laptop screen in Melbourne. That can all be documented and recorded simply by taking a screenshot or a screen movie.

When considering this more carefully, it becomes clear that it is actually a visualisation of the various technological and also human layers that are being traversed in this kind of communication. And these subtleties of mirroring, transparencies and overlapping strata with parts of our portraits were the base for another approach of creating individual portraits which correspond strongly with the above mentioned multiple digital personality. In our view, they constitute a wonderfully apt and beautifully visual metaphor for the multi-layered nature of our times.

Fusion
The most recent developments of *SkypeLab* happened in cooperation with Professor Maira M. Fróes from the Institute Tercio Pacitti of Computational Applications and Research at the Federal University of Rio de Janeiro and artist Cila Mac Dowell. Besides the portrait and the space, we had a focus on objects with strong emotional connection to the portraited students.

Maira Fróes amplified the students during their drawing sessions with biophysical sensors (internet of the body) to complement more and add scientific characteristics to the individual artistic statements.

Extracts of the biophysical data were integrated in the artistic process or added to artworks to induce a fusion between the artistic view of a portrait representing identity, and biometric data related to the individual. With the fusion of these two different approaches of perception we could create new and essential experiments which have and will continue to lead to unique artworks.

Future
What we are not aware of yet, but which could be a next step, is to keep track of the digital traces we leave with this project. We could try to visualize and include the automatically generated data, called data shadow, created by the *SkypeLab* participants, as we did with the biometric data in Rio de Janeiro. And so transform automatically recorded data into intentionally created artworks to continue the playful and engaged way of dealing with the changes of identity within the digitized world.

Information:

SkypeLab is a project in the framework of the Baden-Württemberg-STIPENDIUM for university students - BWS plus, a program of the Baden-Württemberg Stiftung. (see https://www.bw-stipendium.de/en/home/, https://www.bwstiftung.de)

SkypeLab is also embeded in the Reutlingen Research Institute (RRI) and in the RMIT School of Art Reaserch Group Contemporary, Art, Society and Transformation.

SkypeLab has created numerous original outputs like drawings, paintings, screenshots, photographs and movies as well as workshops, exhibitions and presentations in Melbourne, Reutlingen, Shanghai, Boston, Rio de Janeiro and Baranquillo. Two hard cover publications are available [5], [6].

References:
[1] K. Nicolaïdes, *Natural Way to Draw: A Working Plan for Art Study*. London, England: Souvenir Press Ltd, 2008.
[2] B. Edwards, *Drawing on the Right Side of the Brain*. London, England: Souvenir Press Ltd, 1995.
[3] M. McCormick, "Workshop Mapping Ephemeralities," ed. Rio de Janeiro, Brazil: International Cartographic Association (ICA), 2015.
[4] H. Eichinger, A. Kurz, M. McCormick, www.skypelab.org. 2014, retrieved October 2017.
[5] M. McCormick and H. Eichinger, *Skypetrait:Ttranscontinental Faces*. Reutlingen, City of Reutlingen 2013.
[6] H. Eichinger, M. McCormick, *Skypelab:Transcontinental Faces and Spaces*. Bielefeld: Kerber, 2016.

'Identity is not something acquired and fixed once for all time. Identity is made of attributes that are in constant evolution, reshaping itself depending on the individual's experiences and the context in which the individual evolves.', p.18.

SkypeLab 2 - Freya Pitt, Freya Pitt drawing Thea Tromsdorf, 2012, Mixed media.

1 Introduction

Who am I? Who are you? How do you identify me? How do I trust you?

Those universal and fundamental questions related to the characteristics of every being are, since humankind, at the basis of human relationships with the self and with others. They are essential to establish trusted relations, in family, in service, in trade, in society, between nations.

Who are you? What is your identity? How can I trust you?

These questions found elements of answers in personal experiences, information, knowledge and perceptions that one can aggregate about another or about an entity like an organisation or an institution (a bank, a private company, a public service, etc.).

What do I know about you? What can I learn about you? What can I perceive from you?

An elaborated process of aggregation of different kinds of information (personal experience, information and perceptions) enables us to form an image of the other and provides the basis for our decision to trust or not this person, organisation, institution.

This process of identification is crucial and lies in highly physical elements, particularly concerning perceived elements, involving our five senses, predominantly the sight and hearing. Therefore, in a context where physicality vanishes, such as the digital world, the fundamental questions of *Who am I? Who are you? How do you identify me? How do I trust you?* are taking a particular light. Indeed, the growing digital sphere, in which we are everyday more emerged, develops a particular space, virtual by essence, where the traditional physicality of body and flesh, of concrete and bricks, of smiles and frowning eyebrows disappears or changes forms of expression. Thus, the question *'How the digital world influences the construction of our Identity, of our trust?'* is an essential consideration of our time, and the artistic research on digital identities through the *Skypelab* project as described and commented by Henning Eichinger in his account framing the present report is one of many social markers of its importance.

The aim of this report is to provide an eagle-eye view on the concept of identity at the centre of the question, on its contemporary meaning, on the consequences of its translation into the digital and internet connected world, on the results of the analysis of its digital peculiarities and finally on the challenges that Digital Identity poses to the digital citizen in the attempt to manage and protect its attributes with the advent of Internet of Things and blockchain technology.

'Digital identity is required to describe an entity in the physical world within a digital information system.', p.18.

SkypeLab 3 - Georgina Humphries drawing Chantal Rasquin and self-portrait, 2012. Mixed media.

2 From identity to digital identities

Considering the concept of *digital identity*, meaning the concept of identity in the digital age, requires us to consider the concept of *identity* in the first place.

Identity is an extremely commonly used word[1] that paradoxically represents a concept that remains in itself *"a complicated and unclear concept that nonetheless plays a central role in ongoing (societal) debates"*, as stated by Phillip Gleason more than thirty years ago (1983). Despite the increasing and broadened interest in the concept of identity as a research tool in the last decades, this observation is still true today, more than ever even, with the advent of the digitalisation of our society.

Our aim in this section is to provide an overview, as brief as possible, of how the concept of identity is understood and used today and how it translates into the digital world.

2.1 The concept of identity

Who am I? Who are you? What is your identity? What is the most important part of it?

Is it your gender, your age, your social status, your nationality, your values, your beliefs? Is your identity invariable no matter what or does your identity change depending on where you are, with whom you are, with whom you are interacting?

The answers to those questions are clearly depending on many factors and are not straight-forward. In fact, such questions have been at the centre of many thoughts and discussions from philosophers, historians, anthropologists, social scientists since Greek Antiquity in our Western civilisation.

The search for answers constrains us at first to consider the meaning of identity as a concept. Philosophers over time have developed different ideas building upon and/or rejecting the ones of their predecessors.

To cite but a few among the most influential conceptualisations over the last centuries, Descartes, for example, built on Plato's idea the paradigm that we persist (uniquely) because we have a soul (unique in its elements) distinct from our body and persistent (immortal), being close in that with some religions such as Christianity or Buddhism. Hegel rejects the Cartesian philosophy, as for him the mind (Geist) only becomes conscious when it encounters another mind and not *per se*. Nietzsche on his side supposes also that the *Soul* is an interaction of forces, but considers, unlike Descartes, an ever-changing thing leading to the 'Construction of the Soul'. Heidegger, at his turn, considers that people only really form an identity after death that assembles a finite identity out of seemingly infinite meanings socially constructed. (Cambridge Dictionary of Philosophy, 2nd Edition, 1995)

The concept of identity was also central to the previous century's reflections and discussions and in fact it did see an increase of interest in other fields than philosophy. Descriptions, representation of individuals or groups' identity is a central task of psychology, sociology and anthropology, and the publication of the work of psychologist Erik Erikson in the 1950s (Erikson, 1950) and the development of his concept of *identity*

[1] *Identity,* the word appears in late 16th century in the English language (Oxford dictionary) and is one of the 1000 most commonly used words (Collins dictionary)

crisis[2] (1968) constitutes the basis on which the concept of identity as we now know it now derives mainly.

While for example psychologists most commonly use the term *identity* to describe *personal identity, i.e* the qualities, beliefs, personality, looks and/or expressions that make a person (self-identity) or group (particular social category or social group), another discipline has devoted a great deal of attention to identity. Sociologists generally define the overall self as consisting of multiple identities tied to the different roles a person plays in the social world. We will here briefly consider only the sociological conceptualisation of ***identity*** that resumes itself at the **characteristic of people's experiences of the self in society**.

Among the numerous studies in sociology that attempt to define the concept of identity under a sociological perspective (Gleason, 1983; Fearon, 1999; Oyserman D. , 2001; MacInnes, 2004; Oyserman D. E., 2012; Morgan & Morgan, 2010), we choose the work of James Fearon as a basis (1999). We found his approach the most relevant to our work of studying the translation of the concept of identity in a digital and inter-connected context for the starting point he takes in elements of ordinary language as a way to capture the word's current meanings in everyday and social contexts.

The essence of Fearon's analysis is encapsulated in the following statement:

> *The concept of identity we use now refers to either*
>
> *(a) a social category, defined by membership rules and (alleged) characteristic attributes or expected behaviours, or*
>
> *(b) socially distinguishing features that a person takes a special pride in or views as unchangeable but socially consequential, or*
>
> *(c) (a) and (b) at once.*
>
> Extracted from Fearon, 1999, p.36.

This definition recognises in the current usage of the word "identity", two intertwined meanings that lead to a third one.

Let's consider and paraphrase, at first **point (b)** of the definition which might be closer to each of us:

Identity is the aggregation of distinctive elements of an individual (or entity), recognised by others (socially), that make its unicity remarkable. In other words, we consider here the aggregation of elements of an individual that makes him or her unique. What makes you you and me me. For example: demographic and administrative elements: (name, sex, age, place of birth, address, studies, profession, passport or social security numbers, etc.), biometrics elements (colour of skin, hair, eyes, fingerprints, DNA, etc.), but also social elements (hobbies, interests, tastes, opinions, etc.). We are here touching the ***personal identity****, the self* as commonly understood by psychologists as mentioned above.

We turn now our comments on **point (a)** of Fearon's definition. When we think about identity, we may focus on external markers (what we can see), on our biology or physiology, or how we were born; however, it's also important to understand that our identities are comprised of ideas, ideologies, and ways of seeing the world around us. Our

[2] *Identity crisis* refers to the condition of being uncertain of one's feelings about oneself, especially with regard to character, goals, and origins, occurring especially in adolescence as a result of growing up under disruptive, fast-changing conditions." (Erikson, Identity: Youth and Crisis., 1968)

identities, therefore, are socially constructed, and the way we were born, our age, how we look like are only parts of who we are.

The concept of identity covers also a sense of recognition of communalities of elements between individuals that makes them feel a member of groups, social categories of which they follow the codes, rules and expected behaviour. Any socially recognised groups from local to national scale and beyond develops codes, characteristics that their members are socially expected to follow. Each individual, as part of a society and interacting with others, is a member of different social groups recognised by others either by birth, by choice or by circumstances. We are here describing elements of what can be called ***social identity***.

Interestingly, parts (a) and (b) of Fearon's definition find echoes in the work of the French philosopher Paul Ricoeur who introduced the distinction between the *ipse* identity (selfhood, "who am I?") and the *idem* identity (sameness, or a third-person perspective which objectifies identity) (Ricoeur & Blamey, 1995). Paul Ricoeur took the etymology of the word "identity" as a starting point to his reflection. Indeed, the word "identity" comes from the Latin word *identitas* which had a paradoxical double meaning. On one hand, *ipse* or *essentitas*, the essence, the essential characteristic(s) of an individual or an entity and on the other hand, *idem*, the same, the sameness, the communalities between individual and others, or an entity and others.

Finally, Fearon recognises in his **point (c)** that parts (a) and (b) of his definition, that the personal and social identities are closely intertwined, one nourishing the other and vice-versa. Memberships of social groups can indeed mark the personal identity of individuals while elements of personal identity can lead an individual to choose or abandon membership of social groups. Defining the concept of identity as at once, a social category and socially distinguishing features of an individual, means understanding how we fit in (or do not) with other groups of people but also how we consider others fitting (or not) with groups of people.

Fearon's work on ordinary language shows that the coined and intertwined meanings of the Latin origin of the word identity as *ipse* (the self) and *idem* (the same) are present today in our society and are actually affecting deeply our modern consideration of identity in off-line and on-line contexts where social interactions are following completely new and virtual paths, unexplored so far.

To add to Fearon's work, we consider also the work of the Critical Media project of University of Southern California, USC, Annenberg School for Communication and Journalism which resumes the key considerations on the concept of identity in the following way, extracted from *The Critical Media Project* (2015):

- *Identity is a socially and historically constructed concept. We learn about our own identity and the identity of others through interactions with family, peers, organizations, institutions, media and other connections we make in our everyday life.*
- *Key facets of identity—like gender, social class, age, sexual orientation, race and ethnicity—play significant roles in determining how we understand and experience the world, as well as shaping the types of opportunities and challenges we face.*
- *Social and cultural identity is inextricably linked to issues of power, value systems, and ideology.*
- *The media uses representations—images, words, and characters or personae—to convey specific ideas and values related to culture and identity in society.*

We can add also that

- Identity is not something acquired and fixed once for all time. Identity is made of attributes that are in constant evolution, reshaping itself depending on the individual's experiences and the context in which the individual evolves.
- Identity is socially multiple. Depending on the context and the social groups an individual is interacting with, a sub group of elements, part of his/her identity, will be more or less visible, consciously or not, highlighted or on the contrary masked.

Now, if we consider the concept of *identity in a digital world*, all considerations above are still valid as they are, except the point dedicated to media that sees a noticeable evolution.

When considering digital media compared to traditional media, we can add that users of the digital media participate themselves (not only journalists or editorialists as in the case of traditional mass media) to the representations of their own identity and those of 'the connected others' through images that they post online (including selfies) or likes, words that they publish online (blogs, comments, other posts, forums activities, etc.), characters, elements that they render public (personal choices, 'likes', visited websites, shopping choices and preferences, etc.).

To sum up this section we see that, on one hand, the concept of identity and the way to express itself by any individual has been enriched by the digital dimension that our world is taking while on the other hand, the loss for physicality, of traditional benchmarks renders challenging the tasks of identifying the self and the others, particularly the latter which is at the basis of trusted relationships, online as elsewhere (Lewis & Weigert, 1985).

2.2 The concept of digital identity

If literature provides plentiful definitions of *identity*, we also found several definitions of *digital identity*. We selected the following from among them:

1. *"The persona, name or **identity** which some person or organization **creates** and uses in a **digital** environment." Morgan & Morgan (2010)*

2. *"The **identity** that c**reates** each individual **to register** on web 2.0 applications where it is present, sharing, reflecting and binds to other members of your network of contacts." Oliveira & Morgado (2016)*

3. *"**Digital identity** is the data that **uniquely describes** a person **or a thing** and contains information about the subject's relationships." Windley (2005)*

4. *"**Digital identity** is required to **describe** an **entity** in the physical world within a **digital** information system. Besides carrying some identifier, the **digital identity** will be described with the help of attributes or so-called claims."*
   Alnemr, Quasthoff, & Meinel (2010)

5. *"**Digital identity**: generically, a virtual **representation** enabling the user **to interact** in cyberspace, **to project** a personality and **to describe** a personal or professional trajectory, in order **to learn and share information**, such as news, Websites, hobbies, opinions, etc."*
   Haro de Rosario, Caba Pérez, & del Mar Sánchez Cañadas (2014)

6. ***"Digital identity** is the data that uniquely **describes** a person or a thing and contains information about the subject's relationships. The **social identity** that an internet user establishes through digital identities in cyberspace is referred to as online identity." Amenta, Lazzaroni, & Abba (2015)*

7. *"We define the **identity** of an individual as the **set of information** known about that person. With the development and widespread use of digital technologies, humans have been able to communicate with each other without being physically present. **Digital identity** is the means that an entity (another human or machine) can use **to identify** a user in a **digital** world. The aim of **digital identity** is to create the same level of confidence and trust that a face-to-face transaction would generate." Sandrasegaran & Li (2008)*

8. *"**Digital identity** is the means that an entity can use **to identify** themselves in a **digital** world (i.e., data that can be transferred **digitally**, over a network, file, etc.)." Gritzalis & Lambrinoudakis (2008)*

9. *"Any subset of attributes of an individual which are accessible by technical means and identify this individual within any set of individuals. Usually there is no such thing as a '**digital identity**', but several of them."*
   Sandrasegaran & Huang (2009)

When analysing and comparing the meanings of those definitions, what strikes at first are the **verbs** that have been chosen: ***create, register, describe, interact, project, identify, and learn***. In fact, we have deliberately displayed the definitions above in a particular order so to highlight their characteristics and cluster them.

In the first place, *digital identity* seems to be a **personal creation**, initiated by the holder itself as stated by Morgan and Morgan in definition (1). Oliveira and Morgado (2) add a social dimension to this creation which echoes the recognised social dimension of the concept of identity as developed above. Moreover, we can even sense here its social necessity. It also adds another action from the digital identity holder which is the **registration** on the web 2.0 applications.

Definitions (3) to (6) focus on the fact that digital identity is a **description or representation** that uses '*information about the subject's relationships.*' (3) (Windley, 2005)*, 'with the help of attributes or so-called claims'* (4) (Alnemr, Quasthoff, & Meinel, 2010)*.* For Haro de Rosario, Caba Pérez, & del Mar Sánchez Cañadas (2014) in definition (5), the description and representation is at the service of a **projection** of the digital identity holder. It considers then also a part of personal creation but adds the **social context** with the use of the verbs '*to interact* (…) *to learn and share'*. Digital identity is a representation, a projection that has the **social purpose** of interacting, sharing and learning. The social dimension of digital identity is reinforced by Amenta, Lazzaroni, & Abba (2015)*,* definition (6) while building on Windley's definition (3) that already considers '*information about the **subject's relationships'**.*

Moreover and importantly, Windley (2005) considers '***Digital identity** as the data **that uniquely describes** ... '*, a characteristic of unicity that is developed in the last three definitions. Indeed authors see digital identity as a way either to **identify** trustfully **other digital users** (Sandrasegaran & Li, 2008) or an **individual among other individuals** (Sandrasegaran & Huang, 2009) or '*the means that an entity can use **to identify themselves** in a digital world'*. (Gritzalis & Lambrinoudakis, 2008). The last definition

contests the concept of a digital identity's singularity and prefers to consider the plurality of '***digital identities'*** as 'subset of attributes'. This conceptualisation of plurality of '***digital identities'*** is close to the *'partial identities'* developed by (Pfitzmann & Borcea-Pfitzmann, 2010) and cited earlier in this report.

In a second phase, proceeding with our grammatical analysis, we dedicate our attention to the **subjects** and **objects** of those verbs. We can see that the definitions consider the following entity: **user, person, individual, organization, thing, machine and finally entity** they defined or described by **information, set of information, data, attributes, sub-set of attributes.**

> *'Digital identity: generically, a virtual representation enabling the **user** to interact in cyberspace'*
> Haro de Rosario, Caba Pérez, & del Mar Sánchez Cañadas (2014)
>
> *'The persona, name or identity which some **person** or **organization** creates…'*
> Morgan & Morgan (2010)
>
> **'***The identity that creates each **individual**…'*
> Oliveira & Morgado (2016)
>
> '*…uniquely describes **a person** or **a thing'***
> Windley (2005) & Amenta, Lazzaroni, & Abba (2015)
>
> **'***… **Digital identity** is the means that an entity (another human or machine) can use **to identify** a user…'*
> Sandrasegaran & Li (2008)
>
> '***Digital identity*** *is the means that an entity can use **to identify** themselves in a **digital** world'*
> Gritzalis & Lambrinoudakis (2008)

Now, comparing those elements with our starting points, the threefold definition of the concept of identity as developed by Fearon (1999) and the considerations on the concept made by the Critical Media Project (2015), we see that the translation of the concept of identity into the digital context implies the following:

At first, the integration of **objects, machines, things** as subjects of **digital identity,** which is new compared to the concept of identity that considered only persons, institutions or entities made of persons. Here, an internet connected object, just like an individual or an organization, has a digital identity made of recognizable and unique elements. (IP address, digital footprint, etc.)

The starting point of a digital identity of an entity (individual, organization, or thing) is **a construction** initiated either by the entity itself that translates elements of its identity into the digital world in a representation of the self (individual, organization), or by the creator or owner of the connected (thing).

Digital identity, from 'birth', is enriched by elements of its social online interactions. The **'social' dimension** of the construction of the digital identity becomes then the capacity of a digital entity (individual, organization, or thing) to interact with other digital entities and to see its own digital identity being affected, changed, and/or influenced by those interactions.

Digital identity on one hand serves the entity to define and present itself as unique and **identifiable** in the digital world. Nonetheless and challenging this statement, digital identity can be **partial and multiple**. An entity, (individual, organization, or thing) can be

linked to several, partial digital identities, on purpose or not, which challenges the ideal of unequivocal digital identification.

Summing up those elements: for us, **digital identity** becomes **a set of attributes (digital information) linkable to an entity (individual, organization or thing), that is created by the entity itself, enriched by other entities socially interacting with it, deliberately or not, consciously or not, and that allows the recognition of the entity by others as trustable partner of communication and exchange, possibly via identification and authentication.**

Digital identity is therefore still **a description and a recognition of an entity (individual, organization or thing) based on set of attributes; a social construction in constant evolution which is multi-faceted and linkable to virtually an unlimited set of attributes growing with the digital activities of the entity.**

2.3 Attributes, identifiers - identification, authentication

The identity of a person as we have already seen starts at birth and expresses itself through various elements, characteristics that all together constitute an individual and unique experience, contextualised in a particular society. While identity is a volatile, flexible and abstract 'thing', its manifestations and the ways in which it is exercised are often open to view. Identity is made evident through the use of markers or **attributes** such as, traditionally, the body and its movements, language, dress, behaviour and choice of space, whose effect depends on their (social) recognition by other (social) beings or, in the digital world, name, nicknames, login, passwords, pictures, comments whose effect depends on their recognition and identification by other digital entities for a trusted communication.

The **attributes** of one's identity are any characteristics that can be associated to an entity. They are a virtually unlimited set of possible values and their aggregation forms the identity of an entity. Those considerations stay valid for its translation from the concept of identity to digital identity.

The **identifiers** are a particular category of attributes that can provide a variety of linkages to a specific identity and all together can allow the **identification** and ultimately the **authentication** of the identity of an entity. Identifiers such as name, email, password, are commonly used in the digital world for identification and authentication. Defining attributes, identifiers that allow strong identification and authentication, is crucial for building trust in the digital world but it also poses challenges in terms of privacy and anonymity. The categorisation of the attributes is a first necessary step to support this research.

The literature provides several attempts at **categorisation of the different attributes** describing a person (or an entity) in a digital context (Claus & Köhntopp, 2001; Nabeth, 2009; Pfitzmann & Borcea-Pfitzmann, 2010). For example, Thierry Nabeth proposes a categorisation of those attributes according to three different perspectives: *time, function* and *domain* (Nabeth, 2009, p. 45-46). Pfitzmann & Borcea-Pfitzmann (2010) also consider time in the degree of *changeability, variability* and *predictability* of an attribute. Their consideration about information and relationship are themselves close to Nabeth's categorisation based on function and domain. Nai Fovino, Neisse, A., & Muftic (2014, p. 9) chose to categorise the different attributes '*in level of assurance Hard, Medium, Soft, according to the security level adopted in a digital registration and authentication phases*,

i.*e when [an electronic identity] is associated to a target entity [a digital entity, being it a user or a machine]*'. Here again we found elements of categorisation close to Nabeth's categorisation following domain when considering Government area (passports, identity cards, driving licenses, public health insurance cards), Corporate area (customer access, bank accounts, credit cards), Personal area (personal/professional (Business services) sign-on, financial services, social networks (Facebook), business networks (LinkedIn), and many cloud services.

For our own research, we took Nabeth's categorisation following *time, function and domain* as basis. Nonetheless, we revised slightly the last perspective, *domain of application of the attributes* in integrating the sub-categories 'Family', 'Shopping' and 'Culture' and in reorganising the presentation of set of domains starting from the closest to the individual (the family) to the least (the Government). In doing this, we in fact integrate Bronfenbrenner's ecological theory into Nabeth's categorisation. On one hand, if Nabeth recognizes identity as being socially constructed we feel that he misses some essential social dimension of the concept. On the other hand, Bronfenbrenner argues that individuals exist within overlapping ecological systems that are '*a set of nested structures, each inside the next, like a set of Russian dolls*' (Bronfenbrenner, 1979). The first of these structures is the *microsystem*; this is the immediate environment which can be home, community group and work. The *mesosystem* links two different microsystems together, for example the home and work. The third level, the *exosystem*, involves contexts in which individuals are not active participants but which impact significantly on persons' lives. For example, ones' hobby group or workplaces might have an impact on personal identification. Finally, the *macrosystem* is the larger cultural and social context that impacts on the way in which individuals live, such as the political system or cultural values of the society in which they live. In the categorisation of attributes here under we are therefore building on Nabeth's work viewed under the light of Bronfenbrenner's ecological system of social being.

The **categorisation of attributes of identity** becomes then:

Time: the attributes can be categorised by the level of permanence of the information they represent.

- ***Permanent – given*** *to a person and over which it usually has no influence. (e.g. some biological characteristics like gender, eye colour, fingerprint, etc.)*
- ***Permanent – acquired*** *by a person because of some circumstances or because of deliberate actions. (e.g. new qualification, or learning a new foreign language during a stay in a country)*
- ***Persistent – situations*** *that are not permanent but have some permanence in time. (e.g. the address of a person, a job position, social status, marital status,…but also the colour of the hair)*
- ***Transient – very temporary*** *attributes attached to a temporary situation and particular context. (e.g. the geographical position of a person at a given time)*

Function: the attributes can be categorised according to their functional characteristics.

- ***Identification*** *(e.g. name, social security number, password, etc.)*
- ***Location*** *(e.g. geographical location, address, etc.)*
- ***Biological characteristics*** *(e.g. biometrics, age, etc.)*
- ***Personal – psychological*** *(e.g. personality traits, (dis)likes, state of mind, etc.)*
- ***Group – sociological*** *(e.g. membership, social groups, social networks, etc.)*

Domain: the attributes can be categorised according to their application domain/activities in which these attributes are used while considering a part of them as possibly being kept under anonymity.

- ***Family*** *(e.g. role in the family, mother, father, child, etc.)*
- ***Education*** *(e.g. qualification, etc.)*
- ***Work*** *(e.g. employer, title, role, expertise, work context, tasks, network, etc.)*
- ***Leisure*** *(e.g. personal preferences, friends, chosen social groups but also pseudonyms in virtual world, etc.)*
- ***Shopping*** *(e.g. credit card number, shopping website alias, etc.)*
- ***Culture*** *(e.g. language, religion, beliefs, individual choices and interests, etc.)*
- ***Health*** *(e.g. social security number, medical information, etc.)*
- ***Justice and Police*** *(e.g. criminal files and records, etc.)*
- ***Government*** *(e.g. registration information, tax services, etc.)*

An **attribute** can be categorised at the same time following *time, function* and *domain*. For example, the address of a person could be considered:

- *persistent, as to have some permanence in* ***time****.*
- *providing location of a person as* ***function****.*
- *finding a* ***domain*** *of application in providing elements of unique references for Health, Justice and Police, Government.*

This example also shows the high inter-penetrability between domains of application, where one attribute can serve different domains of application at the same time.

Some attributes are enough to be used to identify uniquely an individual, like passport or social security number or IP number, while others, not considered as uniquely individual, when correlated together can still lead to the identification of a unique digital entity. Pfitzmann & Borcea-Pfitzmann (2010) define such a sub-set of attributes of a person (or an entity) as **partial identity** of a person (or an entity).

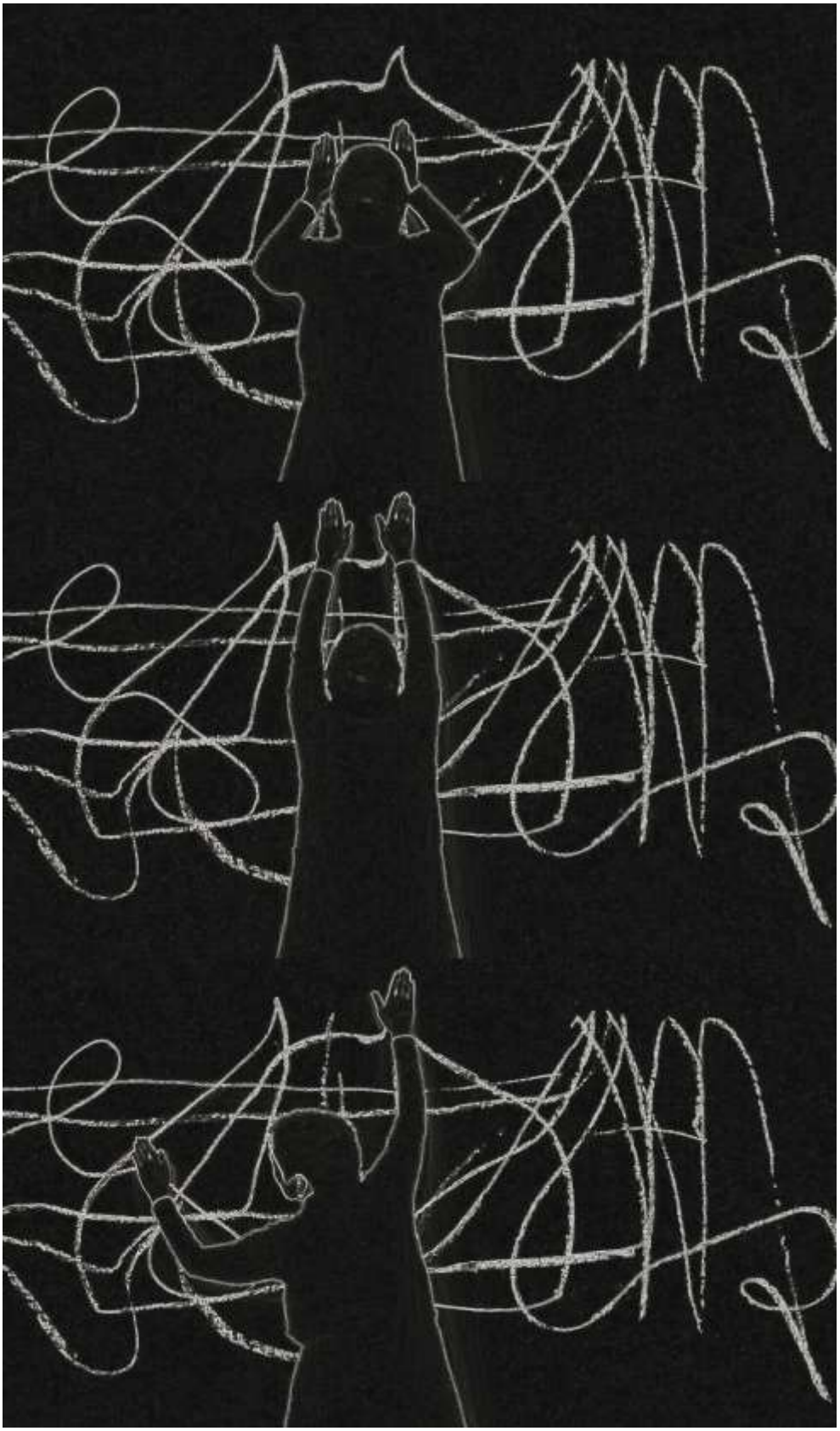
Authentication of identity of a person (or entity) online is yet another step further to anchor trust in an online relationship deprived of physical marks of trust that humankind has used for thousands years. Nai Fovino et al. (2014) building on the components of identity of Aquino & Reed (2002), distinguish three factors of authentication:

- *something the user* ***knows*** *(i.e password),*
- *something the user physically* ***possess*** *(i.e token),*
- *something the user* ***is*** *(i.e biometrics).*

Using one or the other or a combination of two or three of them will provide the level of assurance (Soft, Medium, or Hard) an authentication is looking for. If nowadays most of web services and products request soft authentication via login/email address and password, those services where privacy and confidentiality is key, such as Banks, Health and Administration services typically request stronger authentication measures that rely on more than one authentication measure, password and token or even biometrics, hard authentication when linked to electronic passport for example.

Figure 1-Digital identity - inter-penetrability of domains of attributes. Inspired by Pfitzmann & Borcea-Pfitzmann (2010), Nabeth (2009), Claus & Köhntopp, (2001).

'...digital identity seems to be a personal creation, initiated by the holder itself...', p.19.



SkypeLab 4 - Riza Manalo, Line Dialogue I, 2015. Single channel digital video.

3 Managing digital identity, managing the 'online self'

If digital citizens usually cautiously take care of their passwords, tokens, passport in such exclusive contexts, it seems that attributes linked to soft identification are less taken care of.

Who has not forgotten an online password? How many times did one ask for it to be generated again? No wonder, actually, given the number and variety of services digital citizens access every day via internet, where in theory each access should be protected by different passwords.

Moreover, digital citizens in their everyday communication via emails but also social networks, forum, commercial websites deliberately share and render potentially public personal attributes such as photos including numerous selfies, comments, likes, evaluations, opinions, etc. Any shared online information, but also any online activity itself, constitutes attributes of digital identity that aggregated make it possible to form partial identities that we will call here *soft identities*, that can provide elements of identification and turn into identifiers if not authenticators.

To complete the categorisation of digital attributes as presented in the previous section we can distinguish furthermore two categories of attributes. These are the attributes that we share deliberately, like emails or social network posts, likes, comments, picture including selfies, etc. and the ones that can be inferred by our own online activities, our web behaviour such as online shopping preferences, Youtube or Netflix choices, etc.

The aggregation of attributes linked to the online behaviour of an entity provides elements of profiling that is commonly used nowadays by online service providers to, for example, tailor the information offered to the user to be closest to his/her interest and needs, once those are efficiently profiled.

Here we touch the essential question of the possible private character of digital attributes of an entity. Which attributes among them all are private? Which ones need to be kept private? How? Those questions *in fine* pose the essential question of managing digital identity and the online self.

The aim of this report is not to consider the technical instruments that exist on the market to support the management of digital identity but to consider the elements that in the first place push the digital citizens to share part of their identity with other digital entities.

3.1 Privacy - willingness to share, or not

Like the concepts of *identity* and *digital identity*, the concept of *privacy* has been abundantly and increasingly discussed in the literature in the last two decades. The term *privacy* does not have a worldwide recognised definition and it is open to discussion and to cultural influences. Google Scholar references nearly 400 thousands entries treating the concept of *privacy* since the turn of the century and more than 114 thousands of scientific publications have discussed privacy under one angle or another over the years 2016 and 2017 only (Google Scholar, 2017).

Numerous studies underline the strong privacy concerns that a considerable number of individuals have while using the Internet, as Belanger, Hiller, & Smith (2002) already reported fifteen years ago.

As at the beginning of 2016, in its report on internet use by households and individuals across Europe (Eurostat, 2017), Eurostat marks an increasing diffusion of internet use by European citizens (82%), an increasing use of internet for buying goods or services for private use (55%) and for social networking (52%).

Furthermore, regarding privacy the report (Eurostat, 2017) points out that

> *Disparities between the EU Member States can be observed in the way internet users managed access to their personal information on the internet in 2016. More than one quarter (28%) of EU-28 internet users did not provide personal information over the internet, a share that ranged from just 8% in Luxembourg to half or more in Bulgaria, Portugal and Romania. As such,* ***more than 70% of EU-28 internet users did provide some kind of personal information online, many of them undertaking different actions to control access to this personal information on the internet****. Almost half (46%) of all internet users refused to allow the use of personal information for advertising and two fifths (40%) limited access to their profile or content on social networking sites. In addition, more than one third (37%) of internet users* [claim to] *read privacy policy statements before providing personal information, while just under one third (31%) restricted access to their geographical location.*
>
> *(…)*
>
> *In 2016, 71% of people aged 16-74 in the EU-28 who had used the internet in the previous 12 months knew that cookies can be used to trace people on the internet. Awareness of this issue was slightly higher (74%) among younger users (aged 16–24) and lower (64%) among older users (aged 55–74). Just over one third (35%) of users aged 16-74 reported that they had changed their internet browser settings to prevent or limit cookie use.*

Those data show online shopping and online social networking among the fastest internet growing use in the last years, with an increase of sales in e-commerce of 20% in 2014 worldwide (Ben-Shabat, Nilforoushan, Yuen, & Moriarty, 2015). In the near future the e-commerce growth is expected to overtake the growth of traditional stores as consumers increasingly shift from traditional retail stores to the Internet as a new medium for their shopping processes (Wu & Chou, 2011; Bilgihan, Kandampully, & Zhang, 2016). This trend makes it increasingly important for the actors of the e-economy to provide trustable relationships with their users. Optimum use of privacy and security features combined with trustworthiness are seen as main supporting factors to e-economy growth. Therefore, overcoming and counteracting remaining privacy concerns are seen as key tasks to enable this growth. (Belanger et al., 2002)

Under a psychological prospect, the same Belanger et al. place internet users as consumers for which privacy can be defined as the "*willingness of consumer to share information over the Internet that allows purchases to be concluded*" (Belanger et al., 2002, p.248). Extending this definition to any online communication, basis of most digital activities, **privacy** can be defined as the **willingness of a digital entity (individual, organization, or thing) to share information over the internet to allow a trusted communication**. The choice to share personal information with another online entity is therefore the result of pondered considerations between possible **risks** and **trust** over this entity, being it an individual (user), an organisation (including service provider), or a thing (a machine, an algorithm).

3.2 Privacy, balancing perceived risks and perceived trust

In the physical world, physical elements perceived through the five senses, mainly vision and the hearing but not only, are crucial elements for the deliberation of elements of risks and trust. The recognition of identity attributes of an entity with which one is interacting is therefore central to judge an entity (individual, organization, or a thing) trustworthy. In the virtual world, where by definition elements are virtual and the physicality is reduced to screens, digital users identify elements at the basis of their evaluation of risks and trust at another level.

3.2.1 Perceived Trust

As reported by Lösing (2016, p. 5), Kim, Ferrin and Rao (2008) suggest that digital users base their judgment of a digital entity on four different and complementary forms of trust: *cognition-based, affect-based, experience-based* and *personality-based trust.*

Cognition-based trust is the collection of information about an entity based on observation and perception.

Affect-based trust relates either (1) to second-hand experience reported from other users, or (2) to third-party certification agencies. (1) Just like in the physical world, digital users are influenced by recommendation of friends and family as a sort of social proof of trustworthiness (Seckler et al., 2015; Lim, 2003). Information and references from colleagues, friends and family members are seen as reliable sources of information to avoid a trial and error path already experienced by others (Seckler et al., 2015; Lim, 2003). (2) Third-party seals which certify that an entity meets certain privacy, security and quality standards, see a translation of trust from the certifying entity to the certified entity.

Experience-based trust relies on the personal practice and knowledge of the digital user within the Internet context in general.

Personality-based trust depends on the personal and specific online behaviour styles of each digital user, being it more or less cautious for example, more or less open to risks.

Cognition-based, affect-based, experience-based and personality-based elements of trust all together constitute the first set of information, basis of judgment that a digital entity can built upon another. The second set of information, balancing the first one is made of perceived risks.

3.2.2 Perceived risks

Several studies looked in the last years at defining the perceived risks of users interacting in the new digital environment. Among them, Crespo et al. (2009) conceptualize perceived risk as a multidimensional character, decomposed into financial risk, performance risk, social risk, psychological risk, time/convenience risk and finally privacy risk. Following Lee & Moon (2015) still cited by Lösing (2016, p. 6) financial risks - source risks and transaction security risk - and privacy risks constitute predominantly users' preoccupation and will be solely developed here.

Financial risk regroups risks of two natures, **source risk** and **transactional security risk.**

Source risk is the financial risk at its source as it considers the likelihood of interacting with an untrustworthy entity. Ozpolat et al. (2013) report for example the ease with which it is possible to create new online shops portraying themselves as a high-quality seller on the Internet while masking their real low-quality or even their fraudulent purpose, closing overnight and not delivering goods that have been already paid for.

Transactional security risk sees the other end of financial relationships focusing on the "*manner in which transactions are conducted over the internet*" (Bhatnagar & Ghose, 2004).

Privacy risk is the concerns of a digital user over personal information provided during online interactions and the fear of losing control over given information (Crespo, del Bosque, & de los Salmones Sanchez, 2009). Most online services, starting with free newsletters, emails or social networks, request from the digital user various personal data, like name, surname, email, address and phone number (Kim, Ferrin, & Rao, 2008). Even though by law (Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation, 2016) the collection, storage and management of personal data have to be made under specific rules and conditions in the respect of the users' privacy, the way information will be used can neither be predicted nor controlled (Kim, Ferrin, & Rao, 2008; Glover & Benbasat, 2010). For the time being, given the technology itself, control and security can never reach 100%. This might lead to personal data being distorted or disclosed for sometimes dangerous purposes, like identity-theft (Featherman & Pavlou, 2003; Jia-xin, Hong-xia, & Jun, 2010). Undesirable access and data breach are risks that digital users perceive well.

Beside this intrinsic weakness of the technology, digital users fear the misuse of personal data by third-parties. Third-parties are typically parties with whom the data subject (the digital user) has not agreed directly to provide personal data but with whom the authorised data controller has interactions with including selling database of personal data. The fear is therefore that private information can be used for purposes other than just the initial ones. Risk regarding personal information being disclosed, transmitted, stored and protected can therefore be increased in this context.

Perceived privacy and security protection are the main factors affecting cognition-based trust. Information about products, service, transaction processes and the ability to easily access privacy policies provide an element of trust and reduce the perceived risk (Gefen, Benbasat, & Pavlou, 2008). For example, following (Lim, 2003) the availability of understandable and easily accessible privacy policies are fundamental to increase the trustworthiness of a website.

3.2.3 Balancing perceived risks and perceived trust – comparison of generations

The recent and interesting study (Lösing, 2016) already mentioned focuses on the influence of privacy perception consumers' online behaviour compares two generations of internet users, *Millennials* and *Generation X*. Its research questions were:

(1) How does the perception of risk and trust influence online shopping behaviour?

(2a) How do Millennials and Generation X perceive risk in the online shopping context?

(2b) How do Millennials and Generation X perceive trust in the online shopping context?

(1 + 2) How does the perception of risk and trust influence online shopping behaviour - compared for Millennials and Generation X?

The author fixes the Millennials generation as born between 1992 and 1998, Generation X as born between 1967 and 1981 and describes them respectively on the following terms:

> ***Millennials*** *are [the younger generation which] is expected to become the most educated generation, outranking the older generations' education level (Pew Research, 2010). They are currently either in the beginning of their career, or (…) still in their studies or trainings. They are seen as confident and self-expressive, with strong focus on online social interactions via social networking sites (...) this generation is used to a constant and overloading flow of information. (…) Independence and own thinking is essential, without depending on others in their lifestyle. (…) Their openness to change and upbeat behaviour is based on technological knowledge as [having] grown up with information and communication technologies, like cell phones and online social networks (…). Millennials are seen as "leading technology enthusiasts" (…) as their daily lives [are] mediated by digital technologies, ranging from social interaction, friendship, hobbies over the need to get information about products, services, employers, travel destination and jobs or entertainment possibilities (…). Therefore, mobile devices, laptops and computers are essential for Millennials and are used in a multi-tasking way for almost every activity. (…). They consider their Internet skills as highly sufficient to use the World Wide Web in a comfortable way. (…).*
>
> *Millennials invest a lot of time in researching in order to gain considerable knowledge about latest updates about products and brands online (…). Another important information source for Millennials are online recommendations and (…) reviews, which influence them in their actual (…) behaviour. Besides (…) Millennials are engaging in creating and sharing recommendations online (…). Their open online behaviour and information exchanges underline their continuous access to digital media, since they are highly driven by opinions of friends and users in the virtual world. (…) [L]owest price or highest convenience [matters to] Millennials [which] display very limited loyalty towards brands, but follow more their generational behavioural trends.*
>
> ***Generation X*** *is described as savvy entrepreneurial loners, which currently progress in their career and overtake jobs from Baby Boomers in different economic and political areas (…). They are further described as being independent, as they are born and grown up in an often divorced family situation and in a time where it was usual that both parents worked (…). Although they are described as self-sufficient and self-reliant (…), they care about viewpoints of others in order to reassure their own decisions (…). This attitude can be seen as underlining Generation X's attitude towards risk avoidance, distrust and scepticism (…). Regarding technologies, it is often expected that they are less experienced [than Millennials] when it comes to digital innovations. However, literatures state that GenXers are digitally savvy (…) with having a desire towards web and mail communication. (…)*
>
> *[Among] GenXers there is far less concern about products to display their status or lifestyle (…) However, reading and visiting recommendation sites to reassure their (…) decisions is also essential for this generation (…). Additionally, to make this online (…) generation feel more secure (…), a clear explanation of [online service] products and transaction processes is beneficial (…). Generation X values high-quality products (…).[I]nformation research and trust-assuring information is crucial for this generation. (…) GenXers [show] low capacity for risk, [and preference to] high-quality relationship-enhancing behaviour. Extracts from* (Lösing, 2016, p. 2-4).

In a nutshell, the study presents the following results:

- **Financial risks**, source risks such as unworthy website and transactional security risk, are among the most acknowledged risks and from which digital citizens actively put strategies into place to mitigate. Transaction risk is the only predictor for online behaviour for both generations.
- **Privacy risk** is the main perceived risk for both generations. Yet it is the least 'estimable' risk as the direct consequences of a disclosure of personal data are difficult to perceive if not via emails you never ask for, unless you are under a serious problem of identity theft. Perceived risk can be seen as the only predictor for online behaviour that remains stable as soon as the variable of age is added to the analysis.
- **Difference of perception between *Generation X* and *Millennials*: A paradox between privacy risk perceptions and online safety measures.**

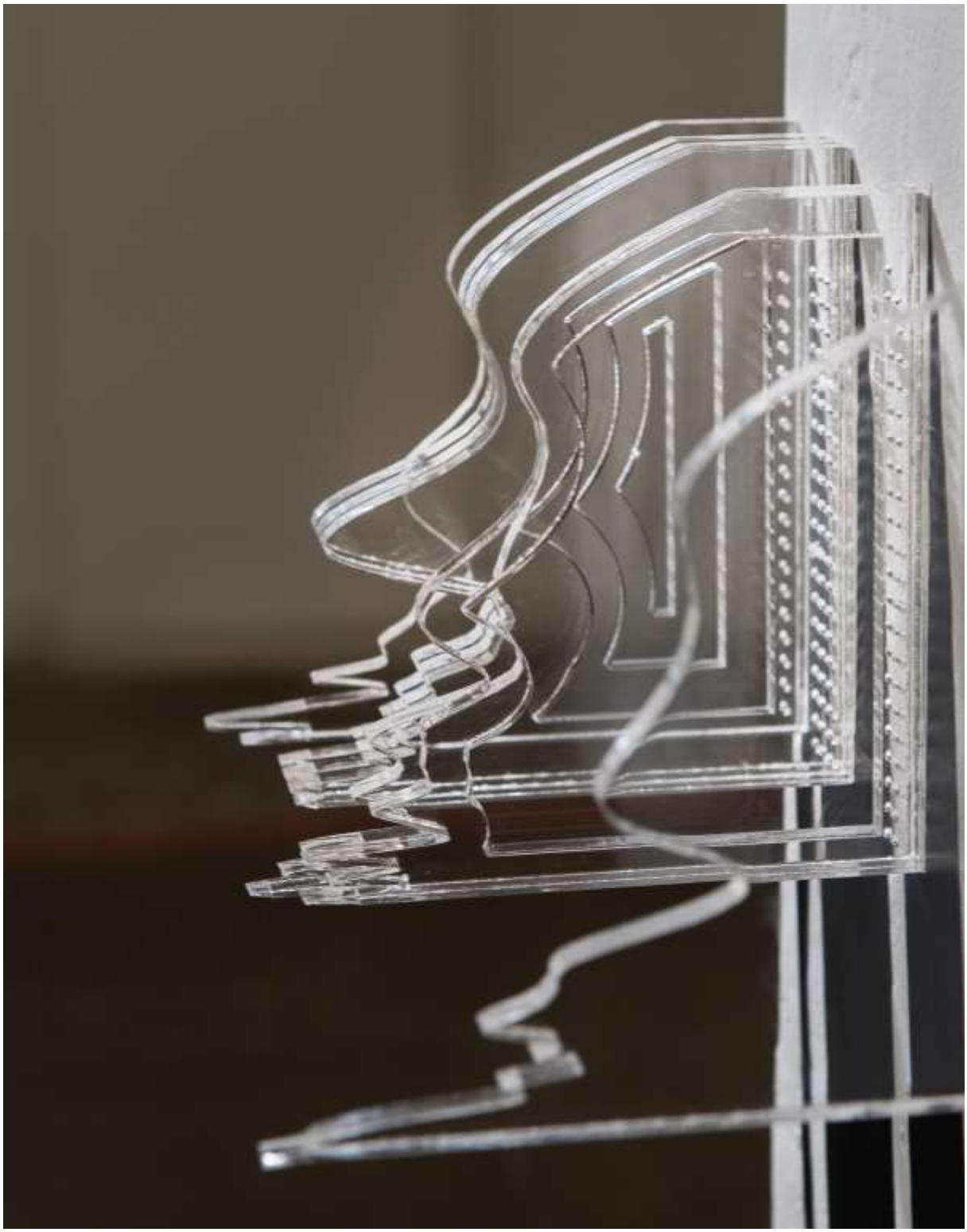
  Millennials perceive more privacy risk probably because they are more social but paradoxically they invest less in protecting their privacy. They feel too safe and confident online while they seem to know less about privacy regulations and tend to rely on others and push the responsibilities on to others, their parents, the GenXers.

  GenXers perceive less privacy risk but invest more in online safety measures than Millennials. They look for time efficiency, trust and quality and rely on reviews and social recommendations.

3.2.4 Going beyond perceived risk, gaining knowledge as basis of trust - a need for education

Another recent study (Golbeck & Mauriello, 2016) that looked at users' concerns and perceptions about privacy, particularly in the context of Facebook apps, reports on the difficulty for the digital users to go beyond their perception of privacy risk without cutting themselves out of digital opportunities. Out of a sample of 120 participants – all digital users; 71 female, 47 male, and two unreported; age ranged from 18 to 66 year-old with an average of 32.3 years and a median of 30; high on the educational background – all report concerns about privacy but are generally under-informed about what data apps could access from their profiles and do not have a full understanding of how that information is shared with the apps. Interestingly, users who reported not to use Facebook apps were significantly more informed about what data those apps could access than subjects who did use Facebook apps. The study found also that overall, viewing information material increases privacy concerns and understanding about what information apps could access, although even after receiving explicit information on the topic, many subjects still did not fully understand the extent to which apps could access their data.

'When considering this more carefully, it becomes clear that it is actually a visualisation of the various technological and also human layers that are being traversed in this kind of communication. (…). In our view, they constitute a wonderfully apt and beautifully visual metaphor for the multi-layered nature of our times.', p.9.



SkypeLab 5 - Grace Leone, Skype Soundscape (detail), 2016. Laser cut perspex, self-adhesive digital printing film.

4 Digital users awareness and education

From the last two studies reported in the previous section, we retain that understanding digital users' concerns is essential to develop efficient awareness raising and prevention tools. Information about privacy measures might not be enough to gain knowledge and competences and to gain trust. Furthermore, education of both digital users and service providers seems essential to tackle the issue of online privacy efficiently and to increase digital users' privacy in general. More work is needed in order to design effective education tools that allows the digital citizens to gain agency regarding their own privacy through new knowledge and skills.

The first part of this section presents a categorisation of privacy risks as a starting point for the digital citizen to go beyond perceptions of the privacy risks, put them into perspective with real risks and gain knowledge and competences to prevent privacy risks or overcome them should they become real issues.

The second part of the section presents the key digital skills that need to be developed by any digital citizen to gain privacy competence with a framework of reference of Digital Competence, the DigComp framework. (Carretero Gomez, Vourikari, & Punie, 2017)

This section builds upon another recent JRC Technical Report entitled 'Privacy safeguards and online anonymity' (Pizzirani et al., 2017). In a world that increasingly requires digital citizens to provide information, including "personal data", to various online services, this report aims to help them to protect and to manage their privacy during online activities through informed technical and educational ways. The report describes the possible threats to online privacy and the legal and technical tools that digital citizens can use to protect themselves against them. The report concludes by highlighting the importance of raising awareness among digital users and empowering them through education, technical and legal tools, such as the General Data Protection Regulation (GDPR) to overcome possible privacy issues. We invite the reader to consult this report for in-depth information. (Pizzirani, Di Gioia, Chaudron, Draper Gil, & Sanchez Martin, 2017)

4.1 Considering privacy risks on informed basis

To address an issue or a threat, it is important first to perceive it, to name it, and then to understand. We here propose the taxonomy developed by (Solove, 2006) as an attempt to categorise, and weigh the issue of privacy risks online in order to provide a tool to understand the phenomenon. Solove's taxonomy is a very detailed categorisation of possible problems related to privacy where he groups the possible harms related to the privacy into four categories:

- **Information Collection**

  Privacy harms: Surveillance, Interrogation.

- **Information Processing**

  Privacy harms: Aggregation, Identification, Insecurity, Secondary Use, Exclusion.

- **Information Dissemination**

  Privacy harms: Breach of Confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion.

- **Invasion**

  Privacy harms: Intrusion, Decisional Interference.

While some of the harms are recognized crimes (e.g. blackmail, appropriation and distortion) that already have specific laws to prevent and punish them, others, instead, become harmful only after a threshold (e.g. surveillance, interrogation) under which otherwise they are considered legitimate if performed by law enforcement agencies following the law and respecting human rights.

Table 1: Solove's taxonomy

A Taxonomy of Privacy Harms (compiled from (Solove, 2006))		
Domain	**Privacy breach**	**Description**
Information Collection	Surveillance	Watching, listening to, or recording of an individual's activities
	Interrogation	Various forms of questioning or probing for information
Information Processing	Aggregation	The combination of various pieces of data about a person
	Identification	Linking information to particular individuals
	Insecurity	Carelessness in protecting stored information from leaks and improper access
	Secondary Use	Use of information collected for one purpose for a different purpose without the data subject's consent
	Exclusion	Failure to allow the data subject to know about the data that others have about him/her and participate in its handling and use, including being barred from being able to access and correct errors
Information Dissemination	Breach of Confidentiality	Breaking a promise to keep a person's information confidential
	Disclosure	Revelation of information about a person that impacts the way others judge its character
	Exposure	Revealing another's nudity, grief, or bodily functions
	Increased Accessibility	Amplifying the accessibility of information
	Blackmail	Threat to disclose personal information
	Appropriation	The use of the data subject's identity to serve the aims and interests of another
	Distortion	Dissemination of false or misleading information about individuals
Invasion	Intrusion	Invasive acts that disturb one's tranquillity or solitude
	Decisional Interference	Incursion into the data subject's decisions regarding its private affairs

4.2 Digital Competences

Education and user awareness are fundamental dimensions of an effective privacy safeguards strategy that links privacy threats to skills and knowledge in order to overcome them.

As also set out in the last Joint Communication to the European Parliament and the Council (European Commission, 2017), the EU needs to affirm a resilient and complete strategy to boost citizen's skills in term of technology, awareness and education, to better place the EU to face cybersecurity and privacy threats.

To respond to this need, already in 2013, a JRC study developed and published a detailed **Digital Competence framework, DigComp** (Brecko, A., Vourikari, & Punie, 2017). This framework, developed with intensive consultation of stakeholders, is tied to needs that every citizen faces while interacting with digital devices and environments. It has become a general reference model for all EU member States for many digital competence initiatives with the aim to create a common language on the development of digital competences. Dedicated frameworks are available for enterprises, teachers, consumers and organisations.

The **DigComp** framework foresees 21 competences (with three proficiency levels), divided into 5 areas, which can be summarised as follows:

1. **Information and data literacy**: To articulate information needs, to locate and retrieve digital data, information and content. To judge the relevance of the source and its content. To store, manage, and organise digital data, information and content.

2. **Communication and collaboration**: To interact, communicate and collaborate through digital technologies while being aware of cultural and generational diversity. To participate in society through public and private digital services and participatory citizenship. To manage one's digital identity and reputation.

3. **Digital content creation**: To create and edit digital content to improve and integrate information and content into an existing body of knowledge while understanding how copyright and licences are to be applied. To know how to give understandable instructions for a computer system.

4. **Safety**: To protect devices, content, personal data and privacy in digital environments. To protect physical and psychological health, and to be aware of digital technologies for social well-being and social inclusion. To be aware of the environmental impact of digital technologies and their use.

5. **Problem solving**: To identify needs and problems, and to resolve conceptual problems and problem situations in digital environments. To use digital tools to innovate processes and products. To keep up-to-date with the digital evolution.

The current version labelled **DigComp 2.1** (Carretero Gomez, Vourikari, & Punie, 2017) focuses on mobile devices, new environments, **data literacy, privacy legislation** and social inclusion (Vourikari, Punie, & Carretero Gomez, 2017).

Other related JRC works enhancing the development of digital competence have as results the following frameworks: **DigCompConsumers** (Brečko, 2017), **DigCompOrg** (Kampylis & Punie, 2016), **DigCompEdu** (Punie & Redecker, 2017)**.**

Table 2: DigComp 2.1

DigComp 2.0 (year 2016)		DigComp 2.1 (year 2017)	
Competence areas (dimension 1)	**Competences (dimension 2)**	**Proficiency levels (dimension 3)**	**Examples of use (dimension 5)**
1. Information and data literacy	1.1 Browsing, searching and filtering data, information and digital content 1.2 Evaluating data, information and digital content 1.3 Managing data, information and digital content	Eight proficiency levels for each of the 21 competences	Examples of use of the eight proficiency levels applied to learning and employment scenario in the 21 competences
2. Communication and collaboration	2.1 Interacting through digital technologies 2.2 Sharing through digital technologies 2.3 Engaging in citizenship through digital technologies 2.4 Collaborating through digital technologies 2.5 Netiquette 2.6 Managing digital identity		
3. Digital content creation	3.1 Developing digital content 3.2 Integrating and re-elaborating digital content 3.3 Copyright and licences 3.4 Programming		
4. Safety	4.1 Protecting devices 4.2 Protecting personal data and privacy 4.3 Protecting health and well-being 4.4 Protecting the environment		
5. Problem solving	5.1 Solving technical problems 5.2 Identifying needs and technological responses 5.3 Creatively using digital technologies 5.4 Identifying digital competence gaps		

4.3 Privacy safeguards and online anonymity in the DigComp

The digital transformation enhances new requirements for digital competences and new vocabulary updates for such competences. Already in its update of 2016 and in its current version the DigComp Area 1 has been updated from "Information" only to "Information and **data literacy**". This to emphasise both the importance of data *per se* and the skills needed to critically evaluate and manage data in a safe and awareness-based way.

Area 4. Safety, section 4.2 has also been moved on from "Protection personal data" to "Protection personal data **and privacy**". This update aims at raising awareness about data privacy as a concept, meaning that data and technology are related to public and legal (Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation, 2016; Glover & Benbasat, 2010) expectations of privacy. According to DigComp, by acquiring digital skills on safety, user is able:

- **To protect personal data and privacy in digital environments**
- **To understand how to use and share personally identifiable information while being able to protect oneself and others from damage**
- **To understand that digital services use a "Privacy policy" to inform how personal data is used**

Privacy and **Data Protection**, **Profiling and targeting**, **behavioural tracking** are extensively analysed in the **DigComp for Consumers**.

'Digital identity is (…) a social construction in constant evolution which is multi-faceted and linkable to virtually an unlimited set of attributes growing with the digital activities of the entity.', p.21.

SkypeLab 6 - Kexin Chen, Polaroid Portrait, 2015. Polaroid photographs

5 Conclusions and future perspective - Identity of Things and Blockchain technology

The concept of identity, its representation and the definition of its attributes indeed see essential changes in their translation into the digital world while the universal questions '*Who am I? Who are you? How do you identify me? How do I trust you?*' remain as essential as before.

In the physical world, physical elements perceived through the five senses are crucial for the process of identification and the deliberation of elements of trust. In the virtual world, the recognition of identity elements or attributes of interactors is even more than before key to invest trust in an interacting entity, being it a person, an organization or a thing.

Our work leads us to reconsider, in section 2, the categorisation of the attributes of Digital Identity and to compose the definition of the latter as *Digital Identity is a set of attributes (digital information) linkable to an entity (individual, organization or thing), that is created by the entity itself, enriched by other entities socially interacting with it, deliberately or not, consciously or not, and that allows the recognition of the entity by others as a trustable partner of communication and exchange, possibly via identification and authentication.*

Furthermore, we recognise that the concept of Digital Identity is still a social construction, in constant evolution, multi-faceted and linkable to virtually an unlimited set of attributes growing with the digital activities of the entity.

In section 3, we saw also that privacy and trust are very closely bound as privacy can be defined as the willingness of a digital entity (individual, organization or thing) to share information over the Internet to allow a trusted communication. The choice to share personal information with another online entity is therefore the result of pondered considerations between possible risks and trust over this entity, being it an individual (user), an organisation (including service provider), or a thing (a machine, an algorithm).

Privacy risk as defined by (Crespo et al., 2009) as the concerns of a digital user over personal information provided during online interactions, and the fear of losing control over given information is mainly a question of perceptions where only information, knowledge and competence can support informed consideration between risks and trust.

Moreover, thanks to Eurostat data and two recent studies looking at users' concerns and perceptions about privacy, (Lösing, 2016) and (Golbeck & Moriello, 2016), we realised that there is no distributed consensus on the concepts of identity and privacy and on the strategies to be enacted to protect them. Diverse generations such as Millennials and Generation X clearly have different perceptions, needs and strategies in the matter. The diversity resides also in its cultural background as we saw rather important disparities between European countries in the way privacy is viewed and protected.

Educating European digital citizens on digital privacy issues and empowering them with efficient and up-to-date digital competences (knowledge, attitudes and skills) is certainly the challenge that our society needs to embrace.

Besides educating digital users to new digital competences, the close future of digital privacy and digital identity see other challenges with the rise of new technologies such as the Internet of Things (IoT) and the Blockchain technology.

Let's consider at first the challenges arising from the advent of the Internet of Things (IoT). One may remember from chapter 2 that digital identity could be defined as the data that

uniquely describes a person or a thing and contains information about the subject's relationships (Windley, 2005).

Indeed, everyday objects such as watch, coffee machine or toothbrush can nowadays be objects connected to the Internet that communicates between them, exchanges data automatically from machine-to-machine with (very) reduced interactions and control from their users and owners.

Also in chapter 2, we saw that each digital entity constructs its own unique Digital Identity made of attributes (data) while growing in relationship with other digital entities. In the case of IoTs, attributes of their identity are also, from the start, from their 'online birth', data belonging to either their constructors, owners and/or users, some of which are personal data, sensitive to privacy risk, such as name or email address, phone numbers, etc. IoTs therefore embed in their own proper Digital Identities attributes of those of their constructors, owners, users, including personal data.

Online security, sees therefore a new challenge to address. How to secure the personal data of flesh and blood people if they become attributes of the Digital Identity of Things?

The second challenge of the Digital Identities of IoTs impacts the elements of Trust as developed in chapter 3. We already see objects or machines becoming independent digital entities each developing their own Digital Identity, responding machines like Alexa or Siri being the most striking examples. The questions that are raised are "How can I trust bits and bytes? Will considerations over cognition-based, affect-based, experience-based and personality-based trust be enough? What other strategies will be needed to ensure trust and privacy in the online world?"

Some put great expectancies in the Blockchain technology to answer this question.

"Blockchain" has seen a rapid integration in the current language in the last months, and yet it remains very much misunderstood. The following definition[3] proposed by Grech & Camilleri (2017) inspired by Piscini e al. (2016) provides a quick introduction to the subject:

> *Simply put, a blockchain is a distributed ledger that provides a way for information to be recorded and shared by a community.*
>
> *In this community, each member maintains his or her own copy of the information and all members must validate any updates collectively.*
>
> *The information could represent transactions, contracts, assets, identities, or practically anything else that can be described in digital form.*
>
> *Entries are permanent, transparent, and searchable, which makes it possible for community members to view transaction histories in their entirety.*
>
> *Each update is a new "block" added to the end of a "chain."*
>
> *A protocol manages how new edits or entries are initiated, validated, recorded, and distributed. With blockchain, cryptology replaces third-party intermediaries as the keeper of trust, with all blockchain participants running complex algorithms to certify the integrity of the whole. (…) Ledgers are tools by which one can determine the owner of an asset at any point in time.*

[3]

Without entering into details we can already see thanks to the words "permanent" "transparent", "trust" of this introduction how the "blockchain technology" could support identification and authentication without suspicion. Will it keep its promises?

The translation of the concept of identity into the digital world opens the door to other deep, complex and crucial questions:

Who shapes our digital identity? Who has control over it? Ourselves, others, organisations, machines?

With the rise of the Internet of Things, where is identity going? What are the consequences? What will be the consequences?

Certainly further research in the field is needed to search for answers.

'The translation of the concept of identity into the digital world opens the door to other deep, complex and crucial questions:

Who shape our digital identity? Who has control over it? Ourselves, others, organisations, machines?', p.43.

SkypeLab 7 - Thi To Uyen Ly, 2015. Textile Prints from Screenshots

References

Alnemr, R., Quasthoff, M., & Meinel, C. (2010). Taking Trust Management to the Next Level. In N. Antonopoulos, G. Exarchakos, M. Li, & A. Liotta, *Handbook of Research on P2P and Grid Systems for Service-Oriented Computing: Models, Methodologies and Applications.* Hervey PA: IGI-Global. doi:10.4018/978-1-61520-686-5.ch034

Amenta, V., Lazzaroni, A., & Abba, L. (2015). Internet Identity and the Right to be Forgotten: International Trends and Regulatory Perspectives in. In M. Boucadair, & C. Jaquenet, *Handbook of Research on Redesigning the Future of Internet Architectures.* Hershey, PA, USA: IGI Global. doi:10.4018/978-1-4666-8371-6.ch002

Aquino, K., & Reed II, A. (2002, Dec). Identity, The self-importance of moral. *Journal of Personality and Social Psychology, Vol 83(6), 83*(6), 1423-1440. doi:http://dx.doi.org/10.1037/0022-3514.83.6.1423

Bacigalupo Margherita, K. P. (2017, 05 10). *Entrepreneurship Competence.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/entrecomp

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The journal of strategic Information, 11*(3), 245-270.

Ben-Shabat, H., Nilforoushan, P., Yuen, C., & Moriarty, M. (2015, April). *Global Retail E-Commerce Keeps On Clicking.* Retrieved from https://www.atkearney.com/consumer-products- retail/e-commerce-index.

Bhatnagar, A., & Ghose, S. (2004). Segmenting consumers based on the benefits and risks of Internet shopping. *Journal of Business Research, 57*(12), 1352-1360.

Bilgihan, A., Kandampully, J., & Zhang, T. (2016). Towards a unified customer experience in online shopping environments: Antecedents and outcomes. *International Journal of Quality and Service Sciences, 8*(1), 102-119.

Brečko, B. F. (2017, 03 20). *The Digital Competence Framework for Consumers.* doi:10.2791/838886

Brecko, B., A., F., Vourikari, R., & Punie, Y. (2017, 04 08). *The Digital Competence Framework for Consumers.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digital-competence-framework-consumers

Bronfenbrenner, U. (1979). *The Ecology of Human Development: Experiments by Nature and Design.* Cambridge, Mass.: Harvard University Press.

Cambridge Dictionary of Philosophy, 2nd Edition. (1995). Cambridge, UK: CUP.

Carretero Gomez, S., Vourikari, R., & Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-21-digital-competence-framework-citizens-eight-proficiency-levels-and-examples-use

Carretero Stephanie, P. Y. (2017, 04 20). *The Digital Competence Framework 2.0.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework

Charalambos Vrasidas, E. C. (n.d.). *MOOCS4inclusion.* Retrieved from MOOCS4inclusion: http://moocs4inclusion.org/

Claus, S., & Köhntopp, M. (2001). Indentity Managements and Its Support of Multilateral Security. *Computer Networks, Special Issue on Electronic Business Systems*, pp. 205-219.

Crespo, A. H., del Bosque, I. R., & de los Salmones Sanchez, M. G. (2009). The influence of perceived risk on Internet shopping behavior: a multidimensional perspective. *Journal of Risk Research, 12*(2), 259-277.

Erikson, E. H. (1950). *Childhood and Society.* New York, NY: Norton. Google Scholar.

Erikson, E. H. (1968). *Identity: Youth and Crisis.* New York: Norton.

European Commission. (2016, 07 01). *PACT — Result In Brief.* Retrieved from Eurpean Commission: http://cordis.europa.eu/result/rcn/155988_en.html

European Commission. (2017). Joint Communication to the European Parliament and the Council - Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. *European Commission - High Representative of the Union for Foreign Aggairs and Security Policy, Final*.

Eurostat. (2017, February). *Digital economy and society statistics - households and individuals.* Retrieved Dec 2017, from Eurostat Statistics Explained: http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals

Fearon, J. (1999). *What is Identity (as we now use the word)?* Stanford, CA: Stanford University.

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e- services adoption: a perceived risk facets perspective. *International journal of human-computer studies*, 451- 474.

FERGUSON Rebecca, B. A. (2017, 01 13). *Research Evidence on the Use of Learning Analytics: Implications for Education Policy.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/research-evidence-use-learning-analytics-implications-education-policy

Gefen, D., Benbasat, I., & Pavlou, P. (2008). A research agenda for trust in online environments. *Journal of Management Information Systems, 24*(4), 275-286.

Gleason, P. (1983). Identifying Identity: A Semantic History. *The Journal of American History, 69*(4), 910-931.

Glover, S., & Benbasat, I. (2010). A comprehensive model of perceived risk of e-commerce transactions. *International journal of electronic commerce, 15*(2), 47-78.

Golbeck, J., & Mauriello, M. L. (2016). User Perception of Facebook App Data Access: A Comparison of Methods and Privacy Concerns. *Future Internet, 8*(9), .

Google Scholar. (2017, 12 17). *Definition of Privacy*. Retrieved 12 17, 2017, from Google Scholar.

Grech, A., & Camilleri, A. F. (2017). *Blockshain in Education.* European Commission, JRC. Luxembourg: Publication Office of the European Union.

Gritzalis, S., & Lambrinoudakis, C. (2008). Privacy in the Digital World. In M. Freire, & M. Pereira, *Encyclopedia of Internet Technologies and Applications.* Herevey PA: ISI-Global. doi:10.4018/978-1-59140-993-9.ch058

Haro de Rosario, A., Caba Pérez, C., & del Mar Sánchez Cañadas, M. (2014). Visibility of the Airport Sector: Web 2.0 and Social Communication Networks. In M. M. Cruz-Cunha, F. Moreira, & J. Varajão, *Handbook of Research on Enterprise 2.0: Technological, Social, and Organizational Dimensions* (Vol. 2). IGI Global. doi:10.4018/978-1-4666-4373-4.ch024

Inamorato dos Santos Andreia, P. Y. (2016, 07 27). *Policy Recommendations for Opening Up Education.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/open-education

Jia-xin, Y., Hong-xia, Z., & Jun, W. (2010). Research on the Advantages and Disadvantages of Online Shopping and Corresponding Strategies. *2010 International Conference on E-Product E-Service and E-Entertainment.*

Kampylis Panagiotis, P. Y. (2016, 07 27). *The Computational Thinking Study.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/computational-thinking

Kampylis, P., & Punie, Y. (2016, 07 27). *European Framework for Digitally Competent Educational Organisations.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcomporg

Kim, D., Ferrin, D., & Rao, H. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Decision Support Systems, 44*, 544-564.

Lee, H. H., & Moon, H. (2015). Perceived Risk of Online Apparel Mass Customization Scale Development and Validation. *Clothing and Textiles Research Journal, 33*(2), 115-128.

Lewis, J., & Weigert, A. (1985, June 01). Trust as a Social Reality. *Social Forces, 63*(4), 967-985. doi:https://doi.org/10.1093/sf/63.4.967

Lim, N. (2003). Consumers' perceived risk: sources versus consequences. *Electronic Commerce Research and Applications, 2*(3), 216-228.

Lösing, T. (2016). How does privacy perception influence online shopping behavior? - A comparison between Millennials and Generation X. *7th IBA Conference, July 1st, 2016.* Enschede, The Netherlands: University of Twente.

MacInnes, J. (2004). The sociology of identity:social science or social comment? *The British Journal of Sociology, 55*(4).

Morgan, K., & Morgan, M. (2010). Ethical Issues in Digital Information Technology. In T. Hansson, *Handbook of Research on Digital Information Technologies: Innovations, Methods, and Ethical Issues.* Harvey PA: IGI-Global.

Nabeth, T. (2009). Identity of Identity. In K. Rannenberg, D. Royer, & A. Deuker, *The Future of Identity in the Information Society, Challenges and Opportunities* (pp. 18-69). Verlag Berlin Heiderlberg: Springer.

Nai Fovino, I., Neisse, R., A., R., & Muftic, S. (2014). *Electronic Soft-Idtities (e-IDs).* Ispra: European Commission, JRC.

Oliveira, N. R., & Morgado, L. (2016). Personal Learning Environments: Research Environments and Lifelong Informal Learning. In D. Fonseca, & E. Redondo, *Handbook of Research on Applied E-Learning in Engineering and Architecture Education.* Hervey PA, USA: IGI-Global. doi:10.4018/978-1-4666-8803-2.ch003

Oyserman, D. (2001). Self-concept and identity. In A. Tesser, & N. Schwarz, *The Blackwell Handbook of Social Psychology* (pp. 499-517). Malden, MA: Blackwell.

Oyserman, D. E. (2012). Self, self-concept, and identity. In M. R. Leary, *Handbook of self and identity* (pp. 69-104). New York : Guilford Press.

Özpolat, K., Gao, G., Jank, W., & Viswanathan, S. (2013). Research note-the value of third-party assurance seals in online retailing: An empirical investigation. . *Information Systems Research, 24*(4), 1100-1111.

PACT project. (2014, 11 14). *PACT Final Conference - Vienna [13-14 November 2014].* Retrieved from PACT Final Conference: http://www.projectpact.eu/

Pfitzmann, A., & Borcea-Pfitzmann, K. (2010). Lifelong Privacy: Privacy and Identity Management for Life. In D. P.-H. Bezzi M., *Privacy and Identity Management for Life. Privacy and Identity 2009. IFIP Advances* (pp. 1-17). Berlin, Heidelberg: Springer. doi:https://doi.org/10.1007/978-3-642-14282-6_1

Piscini, E., Guastella, J., Rozman, A., & Nassim, T. (2016). *Blockchain: Democratized trust. Distributed ledgers and the future of value. .* Deloitte University Press.

Pizzirani, A., Di Gioia, R., Chaudron, S., Draper Gil, G., & Sanchez Martin, I. (2017). *Privacy safeguards and online anonymity.* European Commission. doi:10.2760/30934

Punie, Y., & Redecker, C. (2017, 12 01). *Digital Competence Framework for Educators (DigCompEdu).* Retrieved from European Commission: https://ec.europa.eu/jrc/en/digcompedu

Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation. (2016, may). *Official Journal of the European Union*, 1-88. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Ricoeur, P., & Blamey, K. (1995). *Oneself as Another (Soi-même comme un autre).* Chicago: University of Chicago Press.

Sandrasegaran, K., & Huang, X. (2009). Digital Identity in Current Networks. In *Encyclopedia of Information Science and Technology, Second Edition.* Harvey PA: IGI-Global.

Sandrasegaran, K., & Li, M. (2008). Identity Management. In Y. Zhang, J. Zheng, & M. Ma, *Handbook of Research on Wireless Security.* Harvey PA: IGI-Global.

Seckler, M. H. (2015). Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior, 45*, 39- 50.

Solove, D. J. (2006, January). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*, 477-560.

The Critical Media Project. (2015, November 9). "Who Are You?". Los Angeles, California, CA: USC Annenberg School for Communication and Journalism. Retrieved December 5, 2017, from http://www.criticalmediaproject.org/about/key-concepts/

Vourikari, R., Punie, Y., & Carretero Gomez, S. (2017, 07 15). *DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model.* Retrieved from European Commission: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/digcomp-20-digital-competence-framework-citizens-update-phase-1-conceptual-reference-model

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, 193-220.

Windley, P. J. (2005). *Digital Identity: Unmasking Identity Management Architecture (IMA).* O'Reilly Media inc.

Wu, R. S., & Chou, P. H. (2011). Customer segmentation of multiple category data in e-commerce using a soft-clustering approach. *Electronic Commerce Research and Applications, 10*(3), 331-34.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: http://europea.eu/contact

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

- at the following standard number: +32 22999696, or

- by electronic mail via: http://europa.eu/contact

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU publications
You can download or order free and priced EU publications from EU Bookshop at: http://bookshop.europa.eu. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

KJ-NA-29044-EN-N

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/48837

ISBN 978-92-79-77689-2